Accelerate eCommerce with enhanced transaction security

Digital commerce is the new normal as consumers embrace the safety and convenience of online ordering. With 79% of consumers saying they've placed orders using a restaurant's website or app within the last year, the trend is only expected to continue throughout 2021 and beyond.

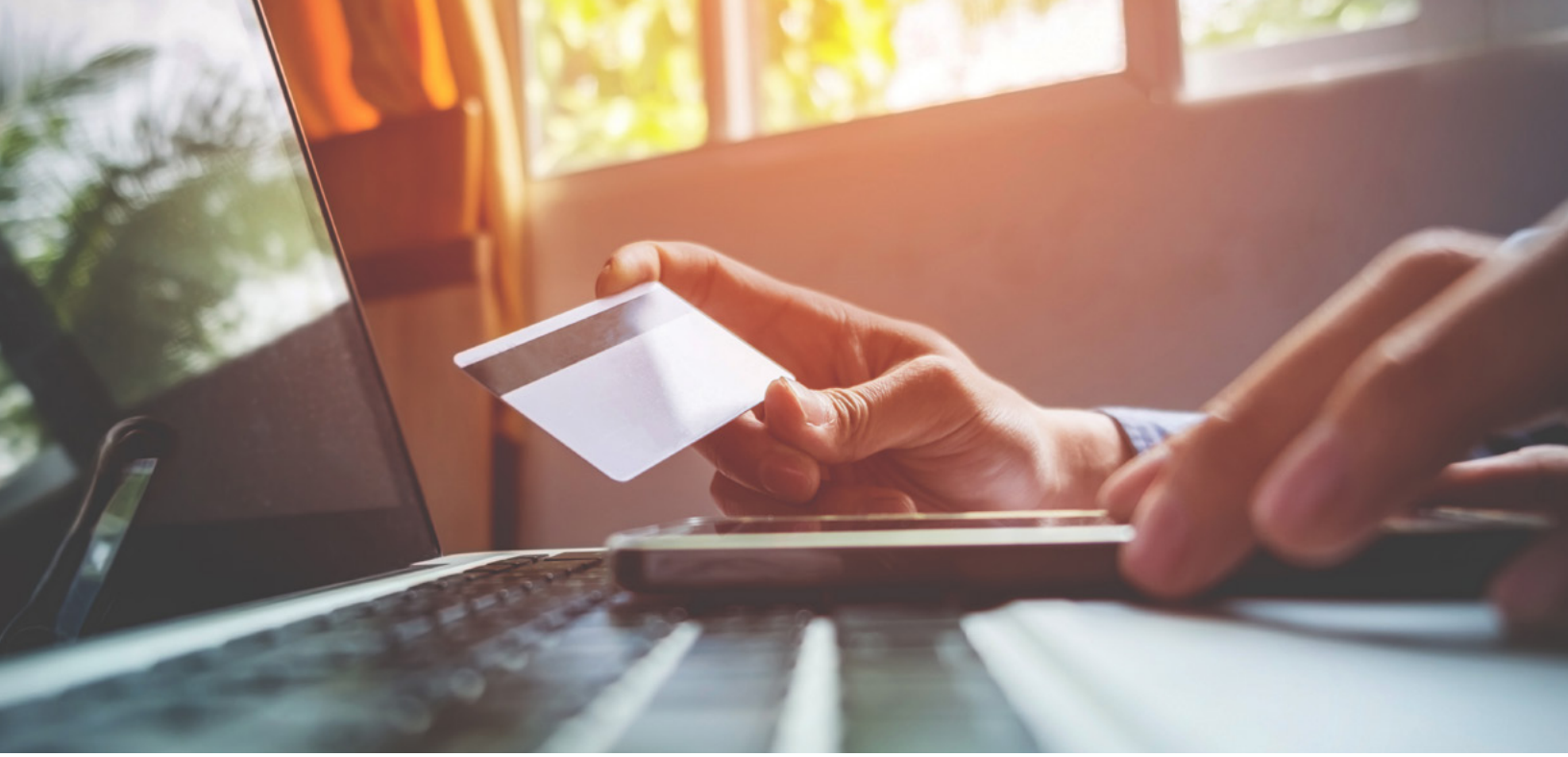
This means that remaining competitive and profitable requires delivering a world-class online customer experience. While many companies might be focusing on loyalty points and digital advertising, one critical aspect restaurants cannot afford to neglect is the authentication of the payment transaction and securing the checkout process.

Since the EMV liability shift in 2015, when the liability for fraudulent losses shifted from the card issuing bank to the business for card-present transactions, payment card fraud has moved online. In the last year alone, experts predict online retail fraud represents a $12 billion problem.

As online sales continue to rise, so too does eCommerce fraud—making securing this channel more important than ever. More than cutting into business revenues, online customers are also being impacted by business rules implemented to help reduce fraud, which can lead to checkout friction, false declines and potentially lost business. The cost of each fraudulent incident is also increasing for businesses.

Fortunately, payment and security technology are constantly innovating to help authenticate online transactions and protect businesses and their payment data. In this white paper, we discuss the most common types of online fraud and how your organization can improve cybersecurity with EMV 3-D Secure, a new tool that speeds up authentication and enhances security while offering shoppers a seamless, faster checkout experience.

usbank | Elavon



Expensive chargebacks top eCommerce fraud

With influx of business being done online every day, new types of sophisticated fraud are affecting businesses across every industry. This includes credential stuffing (mass login attempts to verify stolen accounts), account takeover and streaming potluck (unauthorized sharing of streaming subscriptions).

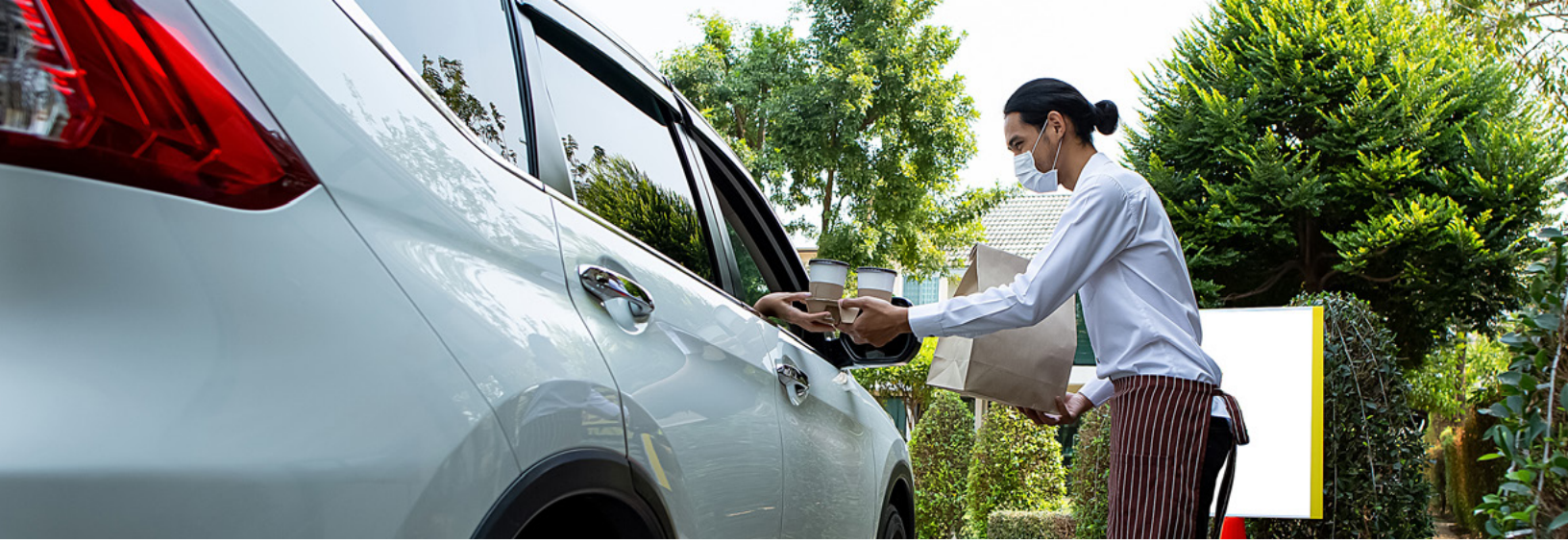
However, the most common result of eCommerce fraud is chargebacks – and it's also one of the most expensive. A chargeback is a transaction disputed by the cardholder or their card issuing bank, which can lead to loss of inventory and additional processing fees. This type of fraud is a significant concern for businesses, as businesses lose around 84% of chargeback disputes.

Chargebacks can happen due to merchant error, criminal fraud or, most often, friendly fraud. This is when a cardholder knowingly (or unknowingly) claims a charge is fraudulent when in fact it was a legitimate transaction.

Friendly fraud can account for up to 75% of all chargebacks, costing businesses both time and money. Although one study showed that 27% of cardholder calls to dispute a charge end up with them realizing they made the purchase, not all cases of friendly fraud are accidental. In fact, 50% of cardholders who successfully commit friendly fraud will do it again within 90 days, according to Chargebacks 911.

With incidents more than doubling between January and June 2020, finding ways to reduce friendly fraud is essential for businesses in today's digital marketplace. Payment security tools that authenticate the transaction before the payment is authorized can help.

usbank | Elavon



Fighting fraud while driving online sales growth

To help restaurants succeed in a competitive digital landscape, payment security tools must do more than safeguard transaction data – they need to help reduce false declines and unnecessary friction that impedes a smooth transaction for customers. This supports a fast, easy and seamless checkout experience that makes it convenient for customers to order online. Frictionless transactions also reduce order abandonment rates, which amounted to about 88% in 2020. According to one Visa study, they found that 95% of transactions were low risk, requiring no additional customer verification.

When evaluating digital payments, it's important to keep the guest experience in mind and make sure your checkout will be user friendly. One tool introduced to fight fraud that failed to make the customer journey a priority was 3-D Secure. Launched in 1999 to help protect cardholder data, 3-D Secure was adopted by all the major card brands. You might recognize it as Verified by Visa or Mastercard SecureCode.

While the tool was effective in fighting fraud, it has not kept up with technological advancements and customer habits like the increased usage of mobile devices. 3-D Secure only works when transactions are presented through an internet browser, which doesn't help transactions that occur through a mobile browser or an app – a major drawback as 43% of consumers use a restaurant mobile app to place online orders.

Another concern is that many issuers require cardholders to use a static password for verification, which is often forgotten and can lead to cart abandonment. If the cardholder enters the wrong password, the bank will decline the transaction. If not already signed up for this process, 3-D Secure will prompt the cardholder to register before continuing with the transaction – one more step that can lead to abandonment.

Overall, 3-D Secure can be frustrating for customers and businesses alike. Fortunately, a new and improved version of the solution is now available that addresses all these issues and more.

usbank | Elavon

Enabling greater authentication with next-gen solutions

Introduced to help drive simple and secure digital payments, EMV 3-D Secure, also known as 3-D Secure 2, offers a smoother user experience and adapts to a wide range of devices. It eliminates static passwords in favor of enhanced authentication points, such as biometrics, that are simple and easy for cardholders to use.

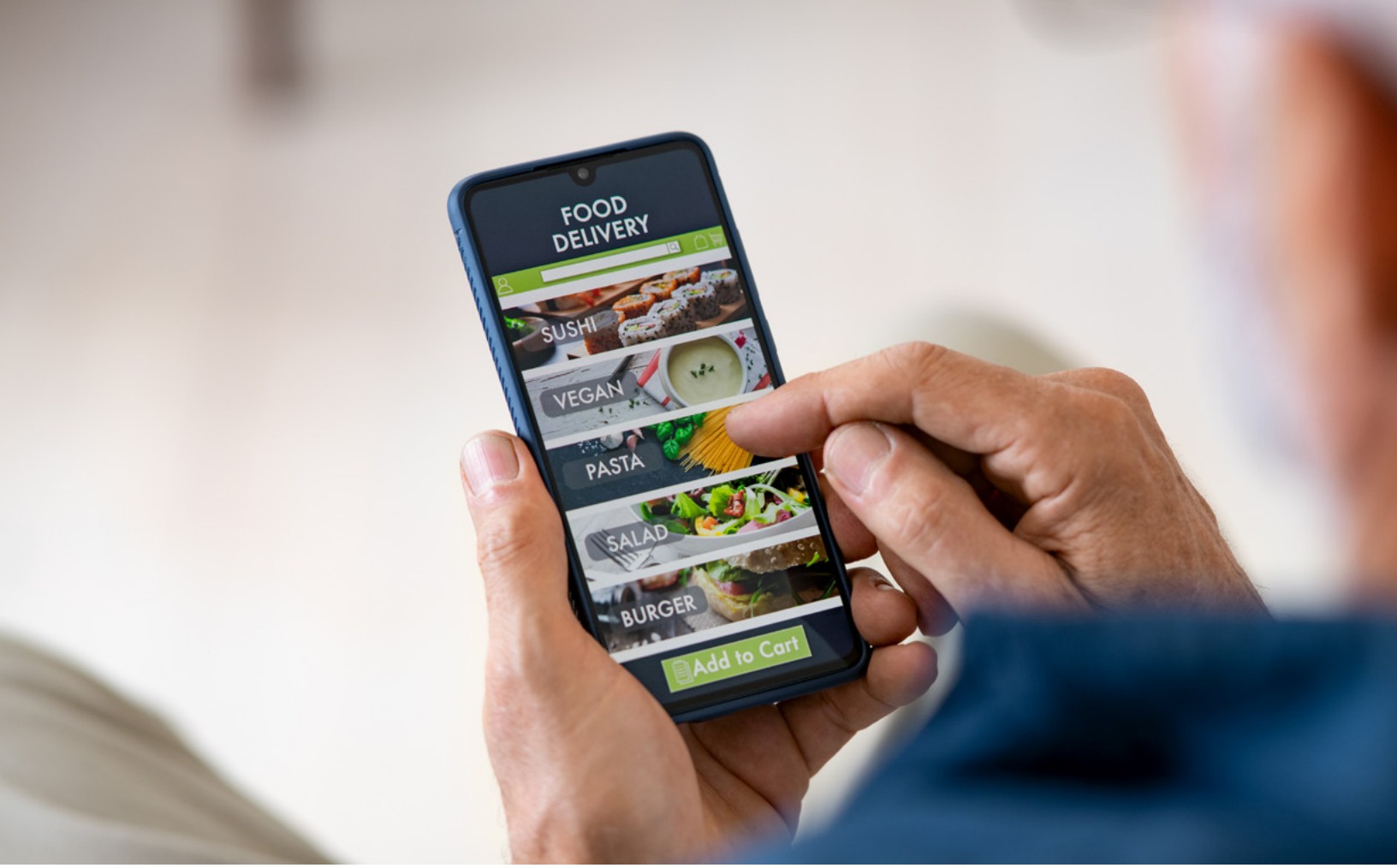
Using 10 times more assessment datapoints than the previous version, EMV 3-D Secure allows for risk-based authentication. After the cardholder submits their information on the restaurant's payment page, it is sent to the issuing bank, which decides if there is enough data to approve the transaction.

When deciding whether to approve and authorize the transaction, card issuers consider several factors, including:

- the dollar amount of the transaction
- whether the cardholder has purchased from that business before
- the cardholder's transaction and behavioral history
- information about the cardholder's device

If the issuer needs more information, the cardholder gets put into a challenge authentication flow. This means that instead of requiring the customer to enter a password that can be easily forgotten, EMV 3-D Secure either prompts for biometric authentication, a one-time use code sent via text message or a security question by the bank. With direct integration into a fraud gateway or through a software development kit (SDK), verification challenges would be native in apps and websites, with no bothersome redirects, popups or iframes required, resulting in a smooth user experience.

The result is a win-win for everyone. Customers enjoy a seamless and secure checkout experience that minimizes unnecessary friction and eliminates the frustration of having to remember and enter passwords. Meanwhile, restaurants help reduce their liability and drive revenue through lowered order abandonment and higher payment authorization rates. Early data insights show a significant positive impact, with businesses using EMV 3-D Secure seeing checkout times reduced by 85% and cart abandonment by 70%.



Adding EMV 3-D Secure to your security suite

Incorporating this essential transaction authentication solution into your digital payments flow is simple with Elavon. Prioritizing cardholder data and merchant protection, we make it easy and affordable to include EMV 3-D Secure for eCommerce payment processing for both mobile and web. To learn more about the benefits of transaction security and how to get started, contact us at getsecure@elavon.com.
